PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-207649
(43)Date of publication of application : 26.07.2002

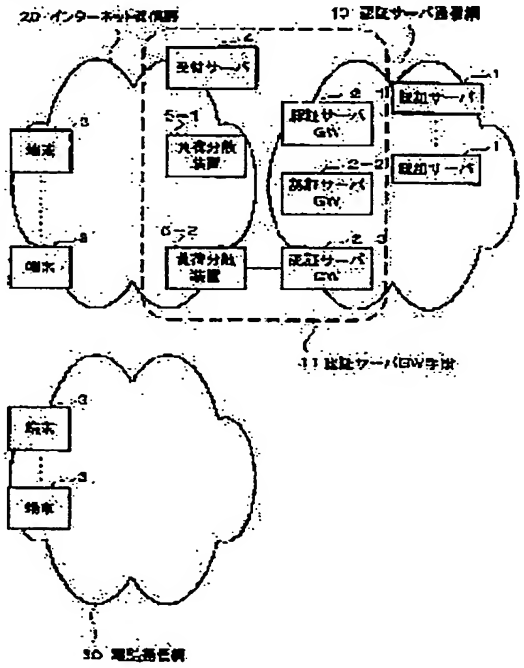
(51)Int.Cl. G06F 13/00
H04M 3/00

(21)Application number : 2001-000060
(22)Date of filing : 04.01.2001

(71)Applicant : NEC CORP
NTT COMMUNICATIONS KK
(72)Inventor : FUJINAMI MASAO
INOUE TAKUYA
MIZOGUCHI YOICHI

(54) INTERNET LOAD-DECENTRALIZED RELAYING CONNECTION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To decentralize the load on a plurality of authentication service GW devices and to make a large number of IPsec connections from dial-up terminals.
SOLUTION: Multiple authentication server GW devices which terminate IPsec are installed, a load decentralizing device which administers the authentication server GW devices (monitors their life/death states is placed), and a reception server is provided so that authentication server GWs are seen from a terminal side as if there were one authenticating server GW. The reception server monitors the life/dead state and use state (number of connections) of the load distributing device to send the address of an authentication server GW back to the terminal.



(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号
特開2002－207649
（P2002－207649A）
(43)公開日　平成14年７月26日(2002.7.26)

(51)Int.Cl.[7]	識別記号	ＦＩ	テーマコード(参考)
Ｇ０６Ｆ　13/00	３５７	Ｇ０６Ｆ　13/00	３５７Ｚ　５Ｂ０８９
Ｈ０４Ｍ　3/00		Ｈ０４Ｍ　3/00	Ｂ　５Ｋ０５１

審査請求　有　　請求項の数６　ＯＬ　（全７頁）

(21)出願番号　特願2001－60(P2001－60)

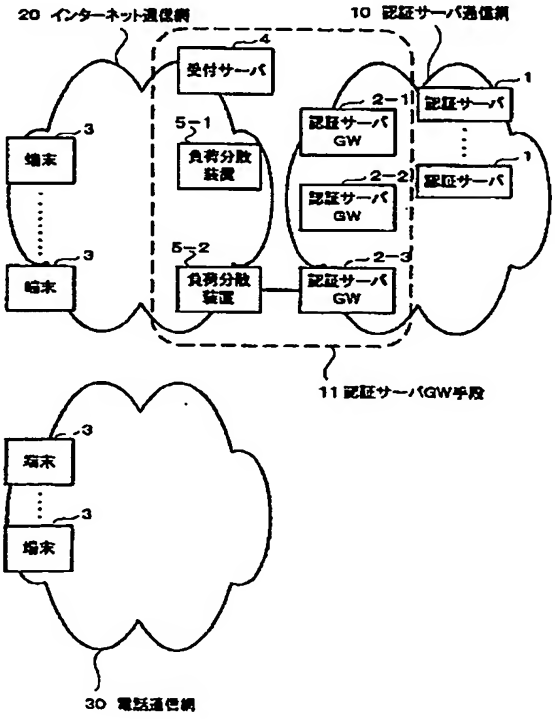
(22)出願日　平成13年１月４日(2001.1.4)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(71)出願人　399035766
エヌ・ティ・ティ・コミュニケーションズ株式会社
東京都千代田区内幸町一丁目１番６号
(72)発明者　藤波　正雄
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100078237
弁理士　井出　直孝　（外１名）

最終頁に続く

(54)【発明の名称】　インターネット負荷分散中継接続方式

(57)【要約】
【課題】　複数の認証サービスＧＷ装置に対する負荷分散を可能にするとともに、ダイアルアップ端末からの膨大な数のＩＰｓｅｃコネクション確立を可能とする。
【解決手段】　ＩＰｓｅｃを終端する認証サーバＧＷ装置を複数台設置し、さらに認証サーバＧＷ装置を取りまとめる（生死状態を監視する）負荷分散装置を置き、さらに、端末側から認証サーバＧＷが一つに見えるように受付サーバを置く。受付サーバは負荷分散装置の生死状態と使用状況（接続数）を監視することによって、認証サーバＧＷのアドレスを端末に返送する。



1

【特許請求の範囲】

【請求項１】　複数の認証サーバを含みインターネット・プロトコル（ＩＰ,internet protocol）に準拠するＩＰアドレスにより制御される認証サーバ通信網（ＣＳＮ, certified server network）とインターネット通信網との接続点に設けられた認証サーバＧＷ（gate way）手段を備え、

この認証サーバＧＷ手段は、インターネット・プロトコルに準拠するアドレスが付与される多数の端末からインターネット通信網を介してアクセス可能なインターネット負荷分散中継接続方式において、

前記認証サーバＧＷ手段は、前記インターネット通信網側からは一つの認証サーバＧＷとして認識される受付サーバと、複数の認証サーバＧＷ装置と、それぞれ前記受付サーバに接続され前記複数の認証サーバＧＷ装置をグループ毎に統括制御する一つまたは複数の負荷分散装置とを含むことを特徴とするインターネット負荷分散中継接続方式。

【請求項２】　前記端末は、電話通信網内にあり、ダイアルアップによりインターネット・プロトコルに準拠するアドレスがその接続の都度付与され、その接続状態が終了したときにはそのアドレスが削除されるアドレス非固定端末を含む請求項１記載のインターネット負荷分散中継接続方式。

【請求項３】　前記受付サーバは、配下の負荷分散装置の動作状態および接続数を管理する手段と、この管理する手段により接続可能な負荷分散装置およびそのアドレスを認識する手段とを含む請求項２記載のインターネット負荷分散中継接続方式。

【請求項４】　前記受付サーバは、前記端末からの問い合わせに対して接続可能な負荷分散装置のアドレスをその端末に対して回答する手段を含む請求項３記載のインターネット負荷分散中継接続方式。

【請求項５】　前記負荷分散装置は、その配下の認証サーバＧＷ装置の動作状態および接続数を管理する手段と、この管理する手段により接続可能な認証サーバＧＷ装置およびそのアドレスを認識する手段と、この手段により認識された接続可能な認証サーバＧＷ装置のアドレスを前記端末に提供する手段とを含む請求項４記載のインターネット負荷分散中継接続方式。

【請求項６】　前記端末は、前記受付サーバからの問い合わせ応答に対応して動作中の認証サーバＧＷ装置に対してインターネット・プロトコルによるセキュリティ接続（ＩＰｓｅｃ）を確立する手段を含む請求項２記載のインターネット負荷分散中継接続方式。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、インターネット通信網から正当な端末であることの認証を受けるために、認証サーバにアクセスする中継接続に利用する。本発明

2

は、ダイアルアップ端末などインターネット・プロトコル（ＩＰ）アドレスが固定的に設定されていない端末から、インターネット・プロトコルにより認証サーバにアクセスするための中継接続に関する。本発明は、きわめて多数の端末が認証サーバにアクセスすることを許容する中継接続に利用する。本発明は認証サーバの負荷分散に関する。

【０００２】

【従来の技術】ユーザがネットワークを介して目的のサービス提供者のサーバに接続し、そのサーバから情報提供その他のサービスを受けるときに、当該サービス提供者のサーバは、サービス提供を求めてきたユーザの正当性を認証し、認証が得られた端末に対して相応のサービスを提供するための技術が知られている。サービス提供者側では、この認証の種類および数に対応して、一つのネットワークの中に認証処理を行う認証サーバを複数設置することが行われている。

【０００３】このような認証処理を行うには、ユーザと認証サーバとの間に、インターネット・プロトコル（ＩＰ）によるセキュリティ接続（ＩＰｓｅｃコネクション）を確立して、他の端末または他の接続から通信内容を盗用されることがないように通信を行う必要がある。また、このようなサービスを求める端末には、固定的なＩＰアドレスが付与されていない端末、たとえば電話通信網からダイヤルアップにより接続を求めるＩＰアドレス非固定端末も含まれる。この場合には、きわめて大量な接続を一時に処理しなければならない場合がしばしば発生する。

【０００４】

【発明が解決しようとする課題】このような従来の認証サービスの課題は、大量の認証要求が発生しているときに、配置されている複数の認証サーバＧＷ装置のうち、どの認証サーバＧＷ装置とＩＰｓｅｃコネクションを確立することが、負荷分散のために合理的であるか判断がつかないことである。すなわち従来方式では、各認証サーバＧＷ装置の稼働または非稼働の状態（生死状態という）は接続制御側で認識できるようになっていない。また各認証サーバＧＷ装置について、それぞれ現時点の接続可能な数が認識できるように構成されていない。したがって、一つの認証サーバに集中的に接続要求が行われる、接続可能な数がきわめて小さい認証サーバに接続可能な数を越える接続要求が行われるなどの状況が発生し、これらの接続要求は接続失敗となり接続要求中の端末が増大することになる。

【０００５】本発明は、このような背景に行われたものであって、複数の認証サーバＧＷ装置の負荷分散を合理的に行うとともに、接続失敗の可能性を小さくすることができるインターネット負荷分散中継接続方式を提供することを目的とする。

【０００６】

【課題を解決するための手段】本発明は、膨大な数のＩＰｓｅｃコネクションに対して、ＩＰｓｅｃを終端する認証サーバＧＷ装置を複数台設置し、さらに複数の認証サーバＧＷ装置を取りまとめ、その生死状態を監視することができる負荷分散装置を置き、さらに、端末側から認証サーバが一つに見えるように受付サーバを置く。そして、受付サーバにより負荷分散装置の生死状態と使用状況（接続数）を監視し、接続可能な認証サーバＧＷ装置のアドレスを接続要求を行う端末に返送する。

【０００７】これにより、複数の負荷分散装置を受付サーバが管理し、端末から受付サーバに接続可能な認証サーバＧＷ装置のアドレスを問合せることができる。受付サーバは、端末からの問合せに対し、認証サーバＧＷ装置のアドレスを回答する。また、認証サーバＧＷ装置の前段に負荷分散装置があるから、端末側には複数の認証サーバＧＷ装置を一台に見せることができる。さらに、受付サーバが認証サーバＧＷ装置の生死状態と使用状況（接続数）を取得して管理し、受付サーバが取得した生死状態と使用状況（接続数）より認証サーバＧＷ装置のアドレスを求める、あるいは、負荷分散装置が認証サーバＧＷ装置の生死状態を認識することもできる。動作中の認証サーバＧＷ装置に対しＩＰｓｅｃコネクションを確立することもできる。

【０００８】すなわち、本発明は、複数の認証サーバ（１）を含みインターネット・プロトコル（ＩＰ，internet protocol）に準拠するＩＰアドレスにより制御される認証サーバ通信網（ＣＳＮ，certified server network）（１０）とインターネット通信網（２０）との接続点に設けられた認証サーバＧＷ（gate way）手段（１１）を備え、この認証サーバＧＷ手段（１１）は、インターネット・プロトコルに準拠する非固定的なアドレスが付与される多数の端末（３）からインターネット通信網（２０）を介してアクセスされるように設定されたインターネット負荷分散中継接続方式であり、本発明の特徴とするところは、前記認証サーバＧＷ手段（１１）は、前記インターネット通信網側からは一つの認証サーバＧＷとして認識される受付サーバ（４）と、それぞれ前記受付サーバに接続され前記複数の認証サーバＧＷ装置をグループ毎に統括制御する一つまたは複数の負荷分散装置（５）とを含むところにある。

【０００９】上記括弧内の数字は後から説明する実施例の図面符号である。これは本発明の構成を理解しやすいように付すものであって、本発明を実施例に限定して理解するためのものではない（以下同じ）。

【００１０】前記端末は、電話通信網（３０）内にあり、ダイアルアップによりインターネット・プロトコルに準拠するアドレスがその接続の都度付与され、その接続状態が終了したときにはそのアドレスが削除される端末を含む構成とする場合にも対応することができる。

【００１１】前記受付サーバ（４）は、配下の負荷分散装置（５）の動作状態および接続数を管理する手段と、この管理する手段により接続可能な負荷分散装置およびそのアドレスを認識する手段とを含む構成とすることもできる。

【００１２】前記受付サーバ（４）は、前記端末からの問い合わせに対して接続可能な負荷分散装置のアドレスをその端末に対して回答する手段を含む構成とすることもできる。

【００１３】前記負荷分散装置（５）は、その配下の認証サーバＧＷ装置の動作状態および接続数を管理する手段と、この管理する手段により接続可能な認証サーバＧＷ装置およびそのアドレスを認識する手段と、この手段により認識された接続可能な認証サーバＧＷ装置のアドレスを前記端末に提供する手段とを含む構成とすることもできる。

【００１４】前記端末（３）は、前記受付サーバからの問い合わせ応答に対応して動作中の認証サーバＧＷ装置に対してインターネット・プロトコルによるセキュリティ接続（ＩＰｓｅｃ）を確立する手段を含む構成とすることもできる。

【００１５】

【発明の実施の形態】本発明実施例のインターネット負荷分散中継接続方式の構成を図１を参照して説明する。図１は本発明実施例のインターネット負荷分散中継接続方式の全体構成図である。

【００１６】本発明は、図１に示すように、複数の認証サーバ１を含みインターネット・プロトコルに準拠するＩＰアドレスにより制御される認証サーバ通信網１０とインターネット通信網２０との接続点に設けられた認証サーバＧＷ装置２－１～２－３を備え、この認証サーバＧＷ装置２－１～２－３は、インターネット・プロトコルに準拠する非固定的なアドレスが付与される多数の端末３からインターネット通信網２０を介してアクセスされるように設定されたインターネット負荷分散中継接続方式である。

【００１７】ここで、本発明の特徴とするところは、複数の認証サーバＧＷ装置２－１～２－３は、インターネット通信網２０側からは一つの認証サーバＧＷ手段１１として認識されるように構成されたところにある。すなわち、認証サーバＧＷ手段１１は、一つの受付サーバ４と、それぞれ受付サーバ４に接続され複数の認証サーバＧＷ装置２－１～２－３をグループ毎に統括制御する一つまたは複数の負荷分散装置５－１、５－２とを含むように構成される。

【００１８】電話通信網３０内の端末３については、ダイアルアップによりインターネット・プロトコルに準拠するアドレスがその接続の都度付与され、その接続状態が終了したときにはそのアドレスが削除される。

【００１９】受付サーバ４は、配下の負荷分散装置５－１および５－２の動作状態および接続数を管理し、接続

可能な負荷分散装置５－ｉ（ｉは１、２のいずれか）およびそのアドレスを認識する。

【００２０】受付サーバ４は、端末３からの問い合わせに対して接続可能な負荷分散装置５－ｉのアドレスをその端末３に対して回答する。

【００２１】負荷分散装置５－１、５－２は、その配下の認証サーバＧＷ装置２－１～２－３の動作状態および接続数を管理し、接続可能な認証サーバＧＷ装置２－ｊ（ｊは１、２、３のいずれか）およびそのアドレスを認識し、認識された接続可能な認証サーバＧＷ装置２－ｊのアドレスを端末３に提供する。

【００２２】端末３は、受付サーバ４からの問い合わせ応答に対応して動作中の認証サーバＧＷ装置２－１～２－３に対してインターネット・プロトコルによるセキュリティ接続（ＩＰｓｅｃ）を確立する。

【００２３】このように、本発明実施例のインターネット負荷分散中継接続方式は、膨大なＩＰｓｅｃを確立するために、認証サーバＧＷ装置２－１～２－３および負荷分散装置５－１、５－２を複数台備え、ＩＰネットワークであるインターネット通信網２０は、端末３、受付サーバ４、負荷分散装置５－１、負荷分散装置５－２で構成される。ＩＰネットワークである認証サーバ通信網１０は、認証サーバＧＷ装置２－１、認証サーバＧＷ装置２－２、認証サーバＧＷ装置２－３および認証サーバ群で構成される。

【００２４】以下に本発明実施例をさらに詳細に説明する。

【００２５】図１において、受付サーバ４は負荷分散装置５－１、負荷分散装置５－２を管理しており、それぞれの生死状態と使用状況（接続数）を取得し管理している。また、負荷分散装置５－１は認証サーバＧＷ装置２－１、認証サーバＧＷ装置２－２の生死状態を負荷分散装置５－２は認証サーバＧＷ装置２－３の生死状態を認識している。

【００２６】端末３がダイアルアップして任意のアドレスを付与され、複数の認証サーバＧＷ装置２とＩＰｓｅｃコネクションを確立する際に、まず、受付サーバ４に認証サーバＧＷアドレスを問合せる。受付サーバ４では、生死状態と使用状況（接続数）により負荷分散装置５のアドレスＩＰ：３を求め応答する。端末３では得られた負荷分散装置５のアドレスＩＰ：３を使用してＩＰｓｅｃ接続要求（認証）を行うと、負荷分散装置５が生死状態を認識し、動作中の認証サーバＧＷ装置２－２に対し振分ける。認証サーバＧＷ装置２－２にてＩＰｓｅｃ認証を行い、許容であればＩＰｓｅｃ接続応答（認証）を返送する。

【００２７】このようにして、本発明では、ダイアルアップした端末３から複数の認証サービスＧＷ装置２－１～２－３を１台に見せ、動作中の認証サーバＧＷ装置２－ｉに対してＩＰｓｅｃコネクションを確立することができる。

【００２８】次に、本発明実施例のインターネット負荷分散中継接続方式の動作を図２を参照して詳しく説明する。図２は本発明実施例のインターネット負荷分散中継接続方式の動作を示すシーケンス図である。受付サーバ４は管理している負荷分散装置５－１および５－２に対し定期的に生死状態および使用状況（接続数）を取得する。また、負荷分散装置５－１では認証サーバＧＷ装置２－１および2－２を監視し、生死状態を認識している。同様に負荷分散装置５－２では認証サーバＧＷ装置２－３を監視し、生死状態を認識している。

【００２９】端末３がダイアルアップし、認証サーバ群とＩＰｓｅｃコネクションを使用して通信するためには負荷分散装置５－１、５－２および認証サーバＧＷ装置２－１～２－３を経由する必要がある。負荷分散装置５－１、５－２および認証サーバＧＷ装置２－１～２－３は複数台あり、端末３ではどの負荷分散装置５－１、５－２および認証サーバＧＷ装置２－１～２－３は動作中であり、使用状況（接続数）が少ないか判断できないため、端末３は受付サーバ４に認証サーバＧＷ装置２－１～２－３のアドレスを問合せる。受付サーバ４では、それぞれの負荷分散装置５－１、５－２の生死状態および使用状況（接続数）を認識しているため、動作中で使用状況（接続数）の少ない負荷分散装置５－１、５－２のアドレスを求め、端末３に負荷分散装置５－１、５－２のアドレスＩＰ：３を返送する。

【００３０】端末３は認証サーバＧＷアドレス問合せで得られたアドレスＩＰ：３に対してＩＰｓｅｃコネクションの接続要求を行う。ＩＰｓｅｃ接続要求（認証）は負荷分散装置５－１で受け、負荷分散装置５－１では認識している認証サーバＧＷ装置２－１、認証サーバＧＷ装置２－２の生死状態より動作中の認証サーバＧＷ装置に負荷分散することで、認証サーバＧＷ装置２－２に転送される。認証サーバＧＷ装置２－２では認証を行い、認証結果が許容であれば、ＩＰｓｅｃ接続応答（認証）で応答する。

【００３１】このように、端末は、受付サーバに問合せて得られたアドレスに接続することになり、複数の負荷分散装置および認証サーバを意識することなく、認証サーバ群に接続ができる。受付サーバは、負荷分散装置の生死状態を監視しているから、端末は死んでいる負荷分散装置に接続することはない。負荷分散装置は、認証サーバＧＷ装置の生死状態を監視しているため、端末は死んでいる認証サーバＧＷ装置に接続することはない。受付サーバと認証サーバＧＷの間に負荷分散することにより、負荷分散装置にて認証サーバの生死状態を監視するから、受付サーバの監視数が減り、ネットワークへの負荷が低減する。受付サーバは、負荷分散装置に対する使用状況（接続数）を監視しているため、負荷の偏った認証サーバＧＷ装置が発生しない。

【００３２】

【効果の説明】以上説明したように、本発明によれば、複数の認証サービスＧＷ装置の負荷分散を可能とし、併せてダイアルアップ端末からの膨大な数のＩＰｓｅｃコネクション確立を可能とすることができる。

【図面の簡単な説明】

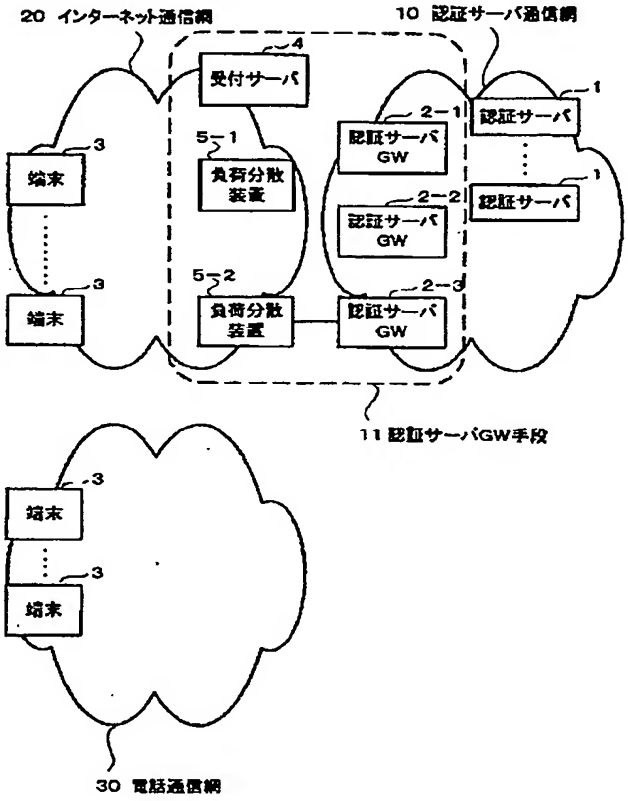
【図１】本発明実施例のインターネット負荷分散中継接続方式の全体構成図。

【図２】本発明実施例のインターネット負荷分散中継接続方式の動作を示すシーケンス図。

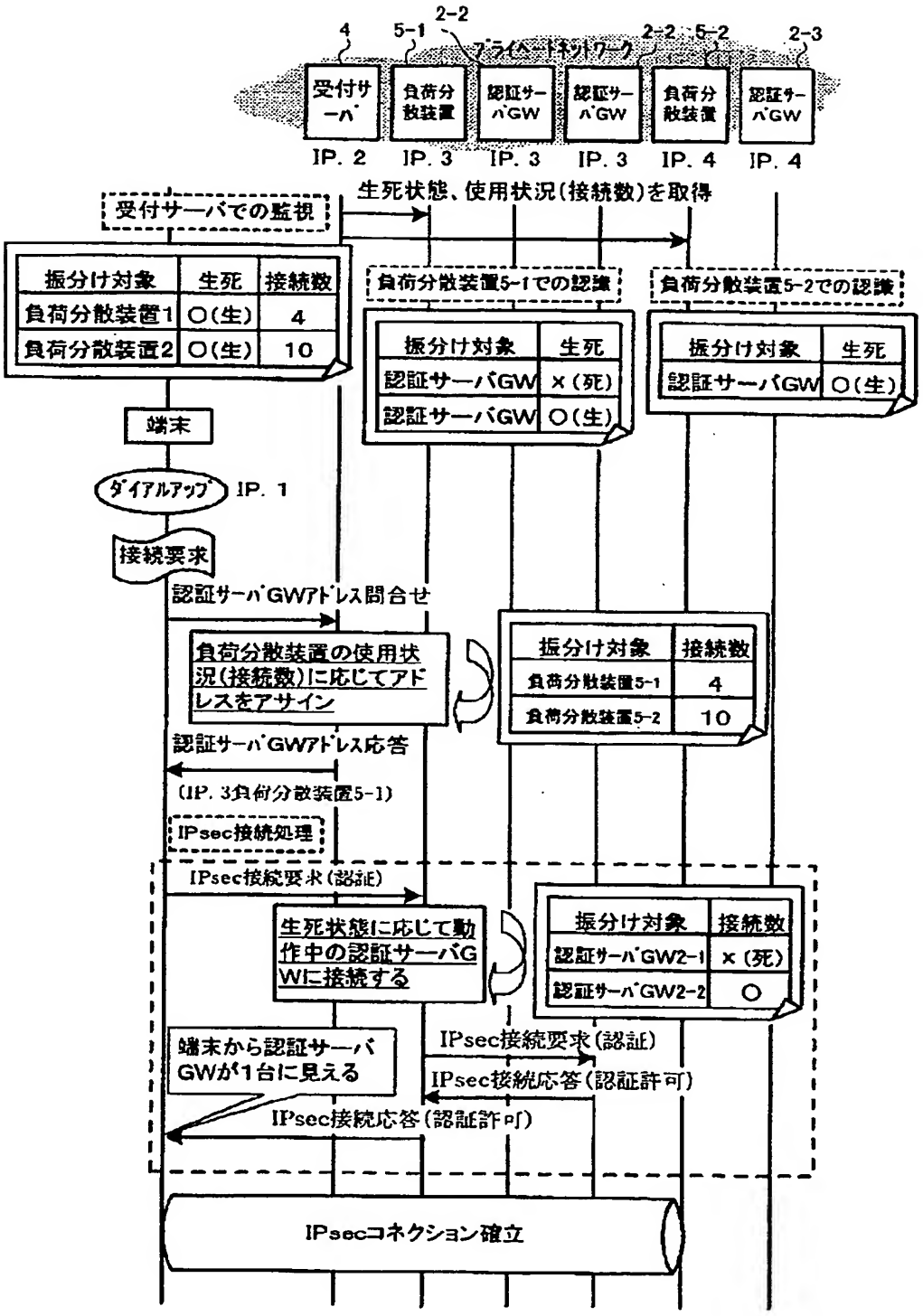
【符号の説明】

１　認証サーバ
２－１～２－３　認証サーバＧＷ装置
３　端末
４　受付サーバ
５－１、５－２　負荷分散装置
１０　認証サーバ通信網
１１　認証サーバＧＷ手段
２０　インターネット通信網
３０　電話通信網

【図１】



【図２】


4
5-1
2-2
2-2
5-2
2-3
プライベートネットワーク
受付サーバ
負荷分散装置
認証サーバGW
認証サーバGW
負荷分散装置
認証サーバGW
IP. 2
IP. 3
IP. 3
IP. 3
IP. 4
IP. 4
生死状態、使用状況(接続数)を取得
受付サーバでの監視
振分け対象 生死 接続数
負荷分散装置1 ○(生) 4
負荷分散装置2 ○(生) 10
負荷分散装置5-1での認識
振分け対象 生死
認証サーバGW ×(死)
認証サーバGW ○(生)
負荷分散装置5-2での認識
振分け対象 生死
認証サーバGW ○(生)
端末
ダイアルアップ IP. 1
接続要求
認証サーバGWアドレス問合せ
負荷分散装置の使用状況(接続数)に応じてアドレスをアサイン
振分け対象 接続数
負荷分散装置5-1 4
負荷分散装置5-2 10
認証サーバGWアドレス応答
(IP. 3負荷分散装置5-1)
IPsec接続処理
IPsec接続要求(認証)
生死状態に応じて動作中の認証サーバGWに接続する
振分け対象 接続数
認証サーバGW2-1 ×(死)
認証サーバGW2-2 ○
端末から認証サーバGWが1台に見える
IPsec接続要求(認証)
IPsec接続応答(認証許可)
IPsec接続応答(認証許可)
IPsecコネクション確立

フロントページの続き

(72)発明者　井上　拓也
東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内

(72)発明者　溝口　陽一
東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内

Ｆターム(参考)　5B089 GA11 GA31 JB16 KA06 KA07 KA12 KB04 KC47
5K051 AA01 BB02 CC01 CC02 FF04 GG02